UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/487,483	01/19/2000	Masue Shiba	04329.2217	3217

22852 7590 07/27/2005

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 07/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/487,483	SHIBA ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *19* is/are allowed.

6)☒ Claim(s) *2-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☑ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 5/6/2005 was received and considered.

2. The IDS of 2/14/2005 was received. The German patent reference to Drescher was considered to the extent that the translated abstract was considered.

3. Claims 2-19 are pending.

Response to Arguments

4. In light of applicant's amendment to the claims, the rejection of claim 11, set forth in the previous Office Action under 35 U.S.C. 112 ¶2 is withdrawn.

5. In light of applicant's amendment to the title, the objection to the specification is withdrawn.

6. For reasons stated in the previous Office Action, claim 19 is allowed and claim 16 stands objected to.

7. Applicant's response (p. 12, ¶3 – p. 13, ¶2) argues that Glaser does not teach an integer based unit arithmetic circuit, a finite field GF(2^m) based unit arithmetic circuit logically adjacent to the integer base unit arithmetic circuit and a selector configured to select one of said integer unit arithmetic circuit and said finite field GF(2^m) based unit arithmetic circuit and a controller controlling said selector to make said selection (Applicant's emphasis). However, Glaser discloses an integer based unit arithmetic circuit/RSA arithmetic processor (Fig. 1, #18) and a finite field GF(2^m) based unit arithmetic circuit/ECC processor (Fig. 1, #20). Glaser further discloses a selector and a controller controlling said selector (Fig. 1, #16 & col. 3, lines 6-14). Specifically, in this section Glaser discloses, "a control signal from control block 16 enables

RSA arithmetic processor 18 for computing the RSA algorithm or ECC arithmetic processor 20 for computing the ECC algorithm". The control signal selects whether the circuit is to perform integer base operations or finite field operations.

8. Applicant's response (p. 13, ¶3 – p. 14, ¶2) argues that Glaser contains two separate unit arithmetic circuits performing independent operations while the control circuit coordinates data transfers. However, Glaser discloses an integer based unit arithmetic circuit/RSA arithmetic processor (Fig. 1, #18) and a finite field GF(2^m) based unit arithmetic circuit/ECC processor (Fig. 1, #20). Glaser further discloses a selector and a controller controlling said selector (Fig. 1, #16 & col. 3, lines 6-14). Specifically, in this section Glaser discloses, "a control signal from control block 16 enables RSA arithmetic processor 18 for computing the RSA algorithm or ECC arithmetic processor 20 for computing the ECC algorithm". Further, Glaser discloses in the integrated circuit embodiment that the INT/POLY signal selects or enables the circuit to generate the mathematical operations of the RSA algorithm and the ECC algorithm (col. 3, lines 25-32) and that the circuit operation changes as a result of the selector signal (col. 4, line 66 – col. 5, line 7). Therefore, the circuits of Glaser are not independently running, each simply received switched operational data. The circuits are being selected by the controller and selection signal to perform operations.

9. Applicant's response (p. 14, ¶3 – p. 15, ¶3) argues that Dworkin fails to disclose a long product-sum operation circuit which executes only polynomial multiplication with a finite field GF(2^m) based polynomial base expression. However, this limitation has not been previously presented and therefore new grounds of rejection are presented. Dworkin discloses that separating the multiply processing and the modulo processing is a naïve approach. However,

Newly cited art to Drescher teaches that using a separate array to perform the multiplication and modulo correction has the benefits of fewer gates (§3.3) and the ability to perform two stage data pipelining (§4.1.2).

Claim Rejections - 35 USC § 112

10. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

11. Claims 11-18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification does not explicitly disclose a long product-sum operation circuit which executes only polynomial multiplication with a finite field $GF(2^m)$ based polynomial base expression.

12. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

13. Claims 11-18 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 11 recites "a controller module configured to divide the processing of modular multiplication into polynomial multiply processing and a modulo". However,

"polynomial multiply processing" is an action and "a modulo" is a number; therefore, it is unclear whether the divide is separating processes or is dividing a value.

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

15. Claims 2-4, 6-7 & 9 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. 6,397,241 to Glaser et al. (**Glaser**).

Regarding claim 2, Glaser discloses an arithmetic apparatus/integrated cryptographic circuit incorporated in a LSI/smartcard (col. 2, lines 1-10) for performing a long integer product-sum arithmetic operation (col. 13, lines 20-33), the arithmetic apparatus/integrated cryptographic circuit comprising an integer based unit arithmetic circuit/RSA arithmetic processor (Fig. 1, #18), a finite field GF(2^m) based unit arithmetic circuit/ECC arithmetic processor logically adjacent to said integer based unit arithmetic circuit (Fig. 1, #20 & col. 1, lines 9-21), and a selector/control configured to select one of said integer unit arithmetic circuit/RSA and said finite field GF(2^m) based unit arithmetic circuit/ECC.

Regarding claim 3, Glaser discloses an adder circuit (Fig. 3), which has a buffer for storing interim result data (Fig. 3, #150, 154, 158), adds the interim result data to result data from one of said integer unit arithmetic circuit and said finite field GF(2^m) based unit arithmetic

circuit which is selected by said selector/INT/POLY (Fig. 3), propagates a carry in an integer based unit arithmetic operation, and propagates no carry in a finite field GF(2^m) based unit arithmetic operation (col. 5, lines 1-7).

Regarding claim 4, Glaser discloses a carry holder (Fig. 3, #152, 156, 160, 162) for storing a carry obtained in a previous cycle/CO, and an output-stage adder circuit configured to add the carry in said carry holder to an output from said adder circuit (Fig. 3, #102), output an upper bit of an addition result as an updated carry/CO to said carry holder, and output a lower bit of the addition result as operation result data/S (Fig. 3).

Regarding claim 6, Glaser discloses an arithmetic apparatus/integrated cryptographic circuit incorporated in a LSI/smartcard (col. 2, lines 1-10) for performing a long integer product-sum arithmetic operation (col. 13, lines 20-33), the arithmetic unit/integrated cryptographic circuit including an integer unit arithmetic circuit/RSA arithmetic processor (Fig. 1, #18), a controller (Fig. 1, #16) configured to output, to said integer unit arithmetic circuit/RSA arithmetic processor, a selection signal for selecting one of an integer unit arithmetic operation/RSA and finite field FG(2^m) based unit arithmetic operation/ECC, and a carry propagation controller (Fig. 1, #16) configured to propagate, when a long product-sum operation is to be executed, a carry of an operation result obtained by said integer based unit arithmetic circuit upon reception of a selection signal corresponding to an integer based unit arithmetic operation, and a propagate no carry of the operation result upon reception of a selection signal corresponding to a finite field GF(2^m) based unit arithmetic operation (col. 5, lines 1-6), wherein an integer based multiply operation and a finite field GF(2^m) based multiply operation is switched by controlling the carry propagation (col. 5, lines 1-6).

Regarding claim 7, Glaser discloses said integer unit arithmetic circuit/arithmetic processor comprising a full adder (FA) (Fig. 7), and said carry propagation controller comprising a switch/gate to which the selection signal and carry out signal are input, and performs carry propagation control of said full adder in units of bits (Fig. 3, #96A).

Regarding claim 9, Glaser discloses adding by propagating a carry when executing the integer based multiply operation (col. 5, lines 1-7 & Fig. 13), and adding without propagating a carry when executing the finite field GF(2^m) based multiply operation (col. 5, lines 1-7 & Fig. 13).

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 5 & 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Glaser**, as applied to claims 2 & 6 above. Glaser does not explicitly disclose encrypting or decrypting, however, the purpose of Glaser's invention is to compute RSA and ECC algorithms (col. 2, lines 1-10) to perform cryptographic functions (col. 1, lines 65-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt and decrypt based on an integer operation and encrypt and decrypt based on a finite field GF(2^m) operation. One of ordinary skill in the art would have been motivated to perform such a

modification to computer ECC and RSA algorithms and perform cryptographic functions, as taught by Glaser (col. 1, lines 65-67 & col. 2, lines 1-10).

18. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Glaser**, as applied to claim 6 above, in further view of "4-bit Multiplier" by **Becker**. Glaser does not explicitly disclose the carry propagation controller comprising a selection section configured to switch between outputting a 2-input EX-OR result obtained by said full adder in units of bits and outputting an EX-OR result based on the result and an input carry as an addition result. However, Glaser discloses that no carries are produced in finite field arithmetic (col. 5, lines 1-7) and that it is necessary to implement carries in integer multiplication (col. 5, lines 1-7) and Glaser implements this in Fig. 3, #96A. Further, Becker teaches that a full-adder works in such a way that the carry is XOR'ed with the partial sum to produce the output (page 4, §4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to switch between outputting just the result (as in finite field math) and outputting the result (sum) XOR'ed with the carry (in integer math). One of ordinary skill in the art would have been motivated to perform such a modification to employ a system that allows switching between integer and finite field arithmetic using Glaser's system, which employs a full adder, as taught by Becker (page 4, §4).

19. Claims 11 & 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,230,179 to Dworkin et al. (**Dworkin**) in view of "VLSI Architectures for Multiplication in GF(2^m) for Application Tailored Digital Signal Processors" by Drescher et al. (**Drescher**).

Regarding claim 11, Dworkin discloses a processor/LSI with an arithmetic unit module/arithmetic processor including a long product-sum operation circuit/ALU (Fig. 4, #34 & #36) which executes a polynomial multiplication with a finite field GF(2^m) based polynomial based expression (col. 4, lines 14-23), and a controller module/controller (Fig. 1, #20) configured to divide the modular multiplication into polynomial multiply processing and a modulo (col. 5, lines 1-10) to cause said long product-sum operation circuit/ALU (Fig. 4, #34 & #36) to execute the polynomial multiplication (col. 5, lines 1-10 & col. 10, lines 18-54). Dworkin further discloses that one approach to polynomial multiplication multiplies A by B, stores the result and then performs the modulo on that result, but lacks the long product-sum operation circuit executing only polynomial multiplication. However, Drescher teaches that using a separate array to perform each of the multiplication processing and modulo correction processing has the benefits of fewer gates (§3.3) and the ability to perform two stage data pipelining (§4.1.2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Dworkin similarly to the described naïve approach and separate the multiply and modulo operations, to pipeline the arithmetic process, as taught by Drescher (§3.3 & §4.1.2). In this situation, the clock controls the division of the modulo processing and polynomial multiplication processing. One of ordinary skill in the art would have been motivated to perform such a modification to pipeline the polynomial and modulo operations to increase throughput, as taught by Hennessy (pp. 437-440, Figs. 6.1 & 6.3).

Regarding claim 17, Dworkin discloses a "processor that combines finite field arithmetic and integer arithmetic", "providing operations required for [elliptic curve] cryptography" (see

col. 1, lines 26-50) and specifically a processor that performs multiplication in a finite field (see col. 4, lines 58-67).

Regarding claim 18, Dworkin discloses an apparatus as described above, comprising a mode selection signal to select integer or finite field arithmetic (see col. 8, lines 10-14). Dworkin further discloses that when performing integer arithmetic, carries are held in register M (see col. 8, lines 15-23).

20. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Dworkin** & **Drescher**, as applied to claim 11 above, in further view of U.S. Patent 4,692,888 to **New**. Dworkin does not explicitly disclose a single precision multiplier and a double precision adder. However, Dworkin discloses that a possible approach is a "brute-force multiply" where the product of the multiplicands (single precision) is 2m bits wide (therefore, to add them, the adder must be 2m bits, i.e. double precision) (col. 10, lines 31-41). Further, New teaches an internal method of product-sum formation (col. 2, lines 1-12). Two numbers are multiplied and stored in a register; two more multiplied and stored in another register. Then the two results are added together (claim 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a single precision multiplier and a double precision adder. One of ordinary skill in the art would have been motivated to perform such a modification to perform a "brute-force multiply" operation, as taught by Dworkin (col. 10, lines 31-41) and to internally compute sum-of-products, as taught by New (col. 2, lines 1-12 & claim 1).

21. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Dworkin**, **Drescher & New**, as applied to claim 12 above, in further view of U.S. Patent 3,064,896 to Carroll et al. (**Carroll**). Dworkin discloses an apparatus performing functions on polynomial coefficients in a finite field as described above, but lacks a method of iterative division as described in claim 13. Carroll teaches a method, and accompanying apparatus for division that allows adequate time for the maximum number of carries and eliminates unnecessary processing (col. 2, lines 1-35). Carroll discloses an apparatus that divides through successive subtractions of the divisor from orders of the dividend until the division is complete and a remainder and all bits of the quotient are produced (col. 1, lines 32-72 and col. 7, lines 35-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Dworkin's apparatus to include iterative division system (modular reduction) as described by Carroll. One of ordinary skill in the art would have been motivated to perform such a modification to eliminate unnecessary processing, as taught by Carroll (col. 1, lines 32-72 and col. 7, lines 35-67).

22. Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Dworkin**, **Drescher**, **New & Carroll**, as applied to claim 13 above, in further view of U.S. Patent 5,468,297 to **Zook**. Dworkin discloses an apparatus that performs modular multiplication, as modified above, but lacks multiplication of an inverse in place of a division operation. Zook teaches that division is a very complex operation in finite field arithmetic, as compared to multiplication, so it is beneficial to perform division by taking the multiplicative inverse of an element followed by a multiplication (col. 1, lines 54-60). Therefore, it would have been

obvious to one having ordinary skill in the art at the time the invention was made to modify Dworkin's apparatus to perform division by first inverting an element then performing a multiplication. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of avoiding a complex division operation, as taught by Zook (col. 1, lines 54-60).

Allowable Subject Matter

23. Claim 19 is allowed.

Conclusion

24. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

(703)746-7239 (for formal communications intended for entry)

Or:

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
June 29, 2005

David Y. Jung
Primary Examiner
7/24/05